



- Bureau of Motor Vehicles
- Emergency Management Agency
- Emergency Medical Services
- Office of Criminal Justice Services
- Ohio Homeland Security
- Ohio State Highway Patrol



Legal Services
1970 West Broad Street
P.O. Box 182081
Columbus, Ohio 43218-2081
(614) 466-7014
www.publicsafety.ohio.gov

September 4, 2019

Freddy Martinez

Via email: 76483-63432700@requests.muckrock.com

Dear Freddy Martinez,

You submitted a public records request in an email received on or about July 1, 2019 to the Ohio Department of Public Safety (DPS).

This request is overly broad. Ohio law provides that a requester has a duty to identify the records sought with sufficient clarity. *State ex rel. Dillery v. Icsman* (2001), 92 Ohio St.3d 312, 314. Please note that your request does not satisfy the requirements of Ohio public records law that a request must be specific and particularly describe what is being sought from the public office. *State ex rel. Zauderer v. Joseph* (1989), 62 Ohio App.3d 752, at 756. This request also constitutes a complete duplication of records and Ohio public records cases have established that public records requests must be more narrowly tailored than a blanket request for all documents of a certain type. *State ex rel. Bristow v. Baxter*, 2018-Ohio-1973, ¶9-13; *See State ex rel. Glasgow v. Jones*, 119 Ohio St.3d 391, 2008-Ohio-4788, ¶ 19. However, in the spirit of cooperation, please find attached to this email records that may be responsive to your request. Certain records have been withheld or redacted in accordance with the following:

- Attorney-client privilege, Ohio Rev. Code § 2317.02; *State ex. Rel. Leslie v. Ohio Hous. Fin. Agency*, (2005) 105 Ohio St.3d 261;
- Homeland Security Records, Ohio Rev. Code § 5502.03(B)(2);
- Confidential Law Enforcement Investigation Records, Ohio Rev. Code § 149.43(A)(1)(h), (A)(2);
- Security Records, Ohio Rev. Code § 149.433.

Please contact me with any questions and should you want to clarify or narrow your public records request. Furthermore, our records retention schedules can be found at <https://apps.das.ohio.gov/rims/Search/PublicSearch.asp> which may assist you in your request.

Sincerely,

Michael Wise

Associate Legal Counsel

Mission Statement

"to save lives, reduce injuries and economic loss, to administer Ohio's motor vehicle laws and to preserve the safety and well being of all citizens with the most cost-effective and service-oriented methods available."

An Equal Opportunity Employer

Records and materials related to the solicitation, acquisition, and use of face recognition technology and related software and services.

This software or services may be provided by Rekognition, Face++, and FaceFirst; this request is applicable to these and any other company providing facial recognition services under consideration or contract with this agency.

Responsive materials include but are not limited to:

- Agreements: contracts (including non-disclosure agreements), licensing agreements, nondisclosure agreements
- Bid records: Requests For Proposal (or equivalent calls for bids), sole source or limited source justification and approval documentation, documentation of selection, and other materials generated in the consideration and selection of the technology in question
- Company relations and communications: records related to meetings or follow-up actions with any vendors, companies, or other private entities marketing face recognition to this agency for immigration, intelligence, law enforcement, or other use.
- Financial records: purchase orders, invoices, and other memoranda and documentation.
- Marketing records: All marketing materials - unsolicited, requested, or otherwise - acquired from vendors of face recognition technology
- Policy records: any policy directives, guidance documents, memoranda, training materials, or similar records governing the use of face recognition technology for immigration, law enforcement, or other purposes. Any memoranda of understanding between this agency and other agencies to share data, access remote systems or other forms of information sharing with external agencies.
- Training records: training material governing the use, sharing, or access to any related data related to or collected by the face recognition software/technology, including the legal standard that is required before using the technology. Documents, should they exist, about training for bias in the use of facial recognition technology.
- Use and function records: Materials that describe the function of the software considered or in use by this agency, including emails, handouts, PowerPoint presentations, advertisements, or specification documents.
- Validation and accuracy: Records, reports, audits, and other documents sufficient to describe validation, accuracy, reliability, and policy compliance of the system.

Please limit the search to records produced from January 1, 2017 – present. Please include in your search as responsive records: communications, memorandums, background papers, meeting minutes, email exchanges, or presentation materials. If your office has questions about this request, please feel free to direct them to the address associated with this request or call the MuckRock office at 617-299-1832.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 business days.

Sincerely,

Freddy Martinez

Filed via MuckRock.com

E-mail (Preferred): 76483-63432700@rcrequests.muckrock.com

Upload documents directly:

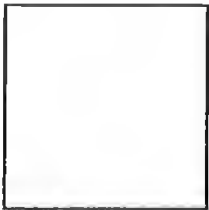
https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fohio-statewide-18057%252Ffacial-recognition-ohio-fusion-center-76483%252F%253Femail%253DSTACC%252540dps.ohio.gov&url_auth_token=AABe7iNqQ3L5X9ix-Ljh5YqdBFw%3A1hiX8p%3AC6RRqFPcQ0GdGb14cFWmczCOVT8

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News
DEPT MR 76483
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



CAUTION: This email was received from an EXTERNAL source, use caution when clicking links or opening attachments.

If you believe this to be a malicious and/or phishing email, please send this email as an attachment to ServiceDesk@dps.ohio.gov

From: Zwayer, Richard

Sent: Monday, July 15, 2019 3:25 PM

To: Huey, Karen <kjhuey@dps.ohio.gov>

Cc: Schmutz, Robin <RSchmutz@dps.ohio.gov>; Quinn, Brian <blquinn@dps.ohio.gov>; Gardner, Brandon <bsgardner@dps.ohio.gov>; Raines, Ronald <RRaines@dps.ohio.gov>; Grayson, Jeffrey <jgrayson@dps.ohio.gov>; Reed Frient, Heather <HRFrient@dps.ohio.gov>

Subject: Facial Recognition

Director Huey,

In all the research OHS personnel, Legal, and I have conducted regarding the HSIN Multi-State Facial Recognition, we have not found any agreement/MOU signed by DPS or OHS.

I have reached out to the MS-FR email account at DHS-HSIN to determine if they enter into any such agreements with states and included a link below with information from their page.

Also, below and attached are the numbers with respect to MS-FR requests completed by OHS and other requests handled by OSP Intel. I also attached a pdf success story that was published by HSIN from the Florida Exchange FC that recognized the STACC in 2018 for our assistance with FR. Let me know if you have any additional questions.

OHS FR Numbers:

2019: 190 requests as of 11 July

- HSIN MSFR-181
 - Ohio LE: 4
 - Out of State LE: 16
 - Federal Agencies: 156
 - FBI: 0
 - Fusion Center Ohio: 1
 - Fusion Center outside Ohio: 4
 - Likely matches made: 10
- Other Requests: 9
 - Out of State LE: 5
 - Fusion Center outside Ohio: 4

2018: 592 Requests

- HSIN MSFR-430
 - Ohio LE: 20
 - Out of State LE: 120
 - Federal Agencies: 233
 - FBI: 5
 - Fusion Center Ohio: 0
 - Fusion Center outside Ohio: 52
 - Likely Matches: 10
- Other Requests: 162
 - FBI: 1
 - Federal Agency: 80
 - Region Fusion Center: 2

- Fusion Center outside Ohio: 2
- Local LE: 2
- Out of State Agency: 77

2016/2017 numbers are based on the teams Facial Recognition Logs/MSFR database search and not Memex. TAU was not using Memex yet for these types of requests. Therefore the breakdown of numbers is not possible.

2017: 419 Requests

- HSIN MSFR-328
 - FBI: 1
 - Likely Matches- 16
- Other Requests: 91

2016: 290

- HSIN MSFR-242
 - FBI: 2
 - Likely Matches- 12
- Other Requests: 48

OSP FR requests over the three years.

OSH (troopers) = 28

Local Ohio PD = 24

Federal = 15

Out of State Agencies = 15

OIU = 4

Task Forces = 4

Ohio Sheriff's Offices = 2

TOTAL = 92

<https://hsin.dhs.gov/Pages/Success%20Stories/Facing-the-Problem-Facial-Recognition-Community-Helps-Investigators.aspx>

Captain Rick Zwayer, Commander

OSP HUB & Statewide Terrorism Analysis & Crime Center (STACC)

2855 West Dublin-Granville Road, Columbus, Ohio 43235

Direct (614) 799-3589

STACC: SAR Tip Line (877) OHS-INTEL

Safer School Tip Line (844) SAFER-OH

OSP Intel (614) 799-6525

OSP Watch Desk (614) 799-6633



2019 FBI Request:
NONE

2018 FBI Requests:

5/9/2018 - MSFR-1481 Case number: IP-79696: crimes against children, **No likely matches** in Ohio based on photos provided. Requestor notified

5/9/2018 - MSFR-1482 Case number: ip-79696: crimes against children, **No likely matches** in Ohio based on photos provided. Requestor notified

10/12/2018 - MSFR-1705 Case number: ip-2997381: The STACC received MSFR-1705 from the FBI regarding a multi-state/country fraud subject:

Title: MSFR-1705

Photo Year: Unknown

Requestor Agency: Federal Bureau of Investigation (FBI)

Requestor ORI: infbiip00

Request Date and Time: 10/12/2018 11:00 AM

Requestor Phone: 2199424722

Case/Incident Number: ip-2997381

Primary Case Type: fraud

Criminal Predicate Narrative: subject is involved with multi state fraud. Could be multi country.

Possible AKA: [REDACTED]

Previous Known Locations: Texas, Arkansas

Request Type: FR Standard Search

A search in OHLEG produced **no likely matches**. The results were sent to the requestor.

11/28/2018 - MSFR-1773 Case number: 497763_CG: Subject has been livestreaming himself making pipe bombs with metal ball bearings. FBI [REDACTED] is investigating. **No likely matches were found.**

12/7/2018 - MSFR-1780 Case number: 496752: [REDACTED] with the FBI sent the STACC a facial recognition request for an individual exhibiting suspicious behavior and possibly conducting preliminary surveillance. The individual has a potential nexus to terrorism and has a previously known location of [REDACTED]. A search in OHLEG produced **no likely matches**. The results were sent to the requestor.

2017 FBI Requests:

5/12/2017 - MSFR-1055 - case number: 305-IP-79696: Crimes against children. Child pornography. Images were run with **no likely matches**.

2016 - 2019 OHLEG FACIAL RECOGNITION SUMMARY

Date	Analyst	Case Number	Agency Type	Purpose	Match Found	Member Entry Number	Comments & Disposition
1/11/2016	Erin Linz		Federal Agencies	Warrant - Homicide	Unknown		Three photos were sent back to Analyst Rost with Pennsylvania State Police
2/2/2016	Wong		OSHP	John Doe Pedestrian hit by vehicle	Not active		Jpr. Dostmer advised of results by Analyst Coulthurst
2/3/2016	Wong		Local Police Departments in Ohio	Fraud	Not active		No matches for fraudulent OH OL photo.
2/8/2016	Wong		Federal Agencies	Homicide/Federal Inactive	Positive		No possible matches provided
3/3/2016	Alyssa Newell		Out of State Agencies	Sex Offense with Juvenile	Not active		No matches, Agent Yarin notified
3/29/2016	Mason		OSHP	EBT Fraud	Not active		No matches on two photos, Analyst Rost notified
4/18/2016	Linz		Out of State Agencies	Remit Fraud	Not active		Jpr. Jackson notified of negative results
4/20/2016	Kirby		Federal Agencies	Identity Theft	Not active		Det. McCoy was notified of negative results - suspects later identified by other means
4/28/2016	Brown		OSHP	Theft	Not active		No active results forwarded to Claudia Miller (Mallory)
5/10/2016	Mason		Local Police Departments in Ohio	Eluding Arrest	Not active		No active results forwarded to Analyst Rost with PSP
5/16/2016	Mason		Out of State Agencies	Drug Offense	Not active		Two possible results emailed to Analyst Rost with Florida Highway Patrol - total 23 checked
1/4/2017	Oodson		Federal Agencies	Larceny/Quick-Chance	Not active		No matches for suspect female
1/23/2017	Mason		Out of State Agencies	Fraud	Positive		No matches for suspect male
1/27/2017	Wong		Local Police Departments in Ohio	COIN Alert - Gahanna PD	Not active		No matches for suspect male
2/9/2017	Wong		Local Police Departments in Ohio	COIN Alert - Grove City PD	Not active		Potential match located and sent to CPO
2/15/2017	Wong		Local Police Departments in Ohio	COIN Alert - Gahanna PD	Not active		PACIC advised of negative results
2/17/2017	Wong		Local Police Departments in Ohio	COIN Alert - Columbus PD	Not active		Jpr. Carr advised of negative results
3/13/2017	Wong		Federal Agencies	Identity Theft	Not active		No matches for suspect male
3/14/2017	Wong		OSHP	Forgery	Not active		Potential match located & sent to Trooper Jarvis, West Virginia State Police
3/17/2017	Michael		OSHP	Terrorism Case - ITF	Not active		No matches for suspect male
3/19/2017	Miller		Out of State Agencies	Commercial Break Ins	Unknown		No matches for suspect male
3/21/2017	Wong		Out of State Agencies	Warrant - Sex Offense	Not active		No matches for suspect male
3/23/2017	Mason		Federal Agencies	Warrant - Drug Trafficking	Not active		Negative results, analyst notified
3/29/2017	Moran		Out of State Agencies	Indecent Exposure	Not active		12 results obtained; no reliable no notification sent at this time
3/29/2017	Ahlborn		Federal Agencies	Escape/Rape/Murder	Not active		5 - No positive matches; result emailed to PACIC on 3/29/17
4/3/2017	Wong		OSHP	Drug Offense	Not active		Negative matches, closed potential match sent to Analyst Bennett for further evaluation
4/11/2017	Wong		Local Police Departments in Ohio	Theft	Not active		Tried to manipulate same photo of suspect for better results; No matches for suspect male
4/12/2017	Moran		Local Police Departments in Ohio	Identity Theft	Not active		No matches for male suspect
5/9/2017	Wong		Out of State Agencies	Identity Theft	Not active		No matches for male suspect
6/1/2017	Mason		OSHP	Robbery	Not active		No matches for male suspect
6/13/2017	Kirby		Federal Agencies	Hit/Slip	Not active		No matches for male suspect
7/2/2017	Moran		OSHP	Pursuit	Not active		No matches for male person of interest
7/9/2017	Wong		Local Police Departments in Ohio	Theft	Not active		No matches for two male suspects
7/24/2017	Wong		Local Police Departments in Ohio	Homicide	Not active		No matches
8/3/2017	Michael		Local Police Departments in Ohio	Crack Seizure / IO Theft in OK	Not active		Possible matches provided to Trooper
8/30/2017	Wong		Federal Agencies	Fraud Case	Not active		0 - Exact match found. Additional photos and info emailed to MI.
9/7/2017	Basom		OSHP	Identity Fraud	Not active		No matches
9/25/2017	Michael		Federal Agencies	Dangerous Offense	Positive		No matches
10/13/2017	Moran		Federal Agencies	Indecent Liberties with a minor	Not active		No matches
11/14/2017	Brower		Local Police Departments in Ohio	Threats to Trooper	Not active		No matches
11/29/2017	Michael		Out of State Agencies	Weapons Offense	Not active		No matches
12/1/2017	Roberts		Local Police Departments in Ohio	Weapons Offense	Not active		No matches returned
12/14/2017	Miller		Out of State Agencies	Attempt to purchase solicited juvenile	Unknown		Possible matches provided to LT Lockhart (WCSO)
1/2/2018	Wong		Local Police Departments in Ohio	IO Theft / Fraud	Not active		No matches
1/10/2018	Robert		Local Police Departments in Ohio	Theft/Stolen Credit Cards	Not active		No matches
2/20/2018	Fahy		Out of State Agencies	Attempt to ID suspect in IO theft / fraud	Not active		No matches
3/4/2018	Miller		OSHP	Weapon Offense	Not active		No matches
3/23/2018	Basom		Out of State Agencies	Dangerous Drugs and Weapon Offense	Not active		No matches
3/27/2018	Wong		Local Police Departments in Ohio	Theft	Not active		No matches
3/29/2018	Bright		Local Police Departments in Ohio	Fraud/IO Theft	Not active		No matches
4/3/2018	Newell		Federal Agencies	Fraud	Not active		No matches
4/12/2018	Oodson/Perez		OSHP	Fraud	Not active		No matches
4/28/2018	Miller		Local Police Departments in Ohio	Felony OVI #1 - 31	Not active		No matches
5/16/2018	Newell		Local Police Departments in Ohio	Robbery	Not active		No matches of witness located
5/22/2018	Wong		OSHP	Missing Person	Not active		Possible matches provided to Detective Gray - none were positive
5/25/2018	Miller		OSHP	Computer Felony	Not active		No matches
6/4/2018	Wong		Local Police Departments in Ohio	Theft	Not active		No matches
6/21/2018	Wong		OSHP	Theft/Fraud	Not active		No matches
6/29/2018	Wong		Local Police Departments in Ohio	Theft	Not active		No matches
7/13/2018	Michael		Local Police Departments in Ohio	Indecent Exposure	Not active		No matches
7/20/2018	Nichols		OSHP	Post 10 Surveillance	Not active		No matches
7/31/2018	Wong		OSHP	Warrant	Not active		No matches
8/8/2018	Newell		OSHP	Pursuit	Not active		No matches
8/13/2018	Wong		Local Police Departments in Ohio	Credit Card Fraud	Not active		No matches
8/30/2018	Armstrong		OSHP	Flight to avoid arrest	Not active		No matches
9/14/2018	Haugenby		Local Police Departments in Ohio	Theft by Deception	Not active		No matches
9/17/2018	Bright		Federal Agencies	Narcotics	Negative		Possible match provided to Analyst Delle Gmont were positive



FACE RECOGNITION POLICY

For Use in Intelligence and Investigative Activities

A. BACKGROUND AND PURPOSE

1. Face recognition (FR) technology involves the ability to examine and compare distinguishing characteristics of a human face contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons.
2. The purpose of this policy ("FR Policy") is to provide STACC/SAIC personnel, who are authorized by the STACC/SAIC to request information from a FR system, with guidelines and principles for the access, use, dissemination, retention, and purging of FR images and related information to ensure that the data is used for official law enforcement or homeland security purposes only and the privacy, civil rights, and civil liberties (P/CRCL) of individuals will not be violated.
3. The STACC/SAIC may only access FR data for official law enforcement or homeland security purposes, including but not limited to:
 - (a) A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity;
 - (b) An active or ongoing criminal or homeland security investigation;
 - (c) To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means;
 - (d) To assist in the identification of a person who lacks capacity or is otherwise unable to identify himself/herself (e.g., incapacitated, deceased);
 - (e) For comparison to determine whether an individual may have obtained one or more official state driver's licenses or ID cards that contain inaccurate, conflicting or false information;
 - (f) To assist in the identification of potential witnesses or victims of violent crime;
 - (g) To support law enforcement in critical incident responses.

B. APPLICABILITY AND LEGAL COMPLIANCE

1. The STACC/SAIC will provide a copy of the FR Policy to each STACC/SAIC employee who will be requesting FR data and will require the employee to provide written acknowledgement of receipt and agreement to comply with the FR Policy. The employee must also complete FR training as directed by the STACC/SAIC. Once both conditions are met, the employee will be a "STACC/SAIC authorized user," permitted to request and receive FR data in accordance with the provisions of the FR Policy.
2. STACC/SAIC authorized users will comply with the FR Policy in their receipt, use, dissemination, retention, and purging of FR images and related information, as well as complying with the applicable laws and policies of Ohio (including, but not limited to, R.C. §§109.57, 149.43, 149.433, 1347.01-1347.15, 2953.32, 2953.52, 5502.03, 5503.10), federal law (e.g., 28 CFR Part 23, Privacy Act of 1974), the Ohio Constitution (e.g., Article I, §§1, 3, 4, 11), and the US Constitution (e.g., Bill of Rights, 1st, 2nd, 4th, 5th, 14th Amendments).

C. GOVERNANCE AND OVERSIGHT

1. The STACC/SAIC Operations Commander or Designee or OHS Security Manager or Designee will designate a senior officer to:
 - (a) Oversee and administer the STACC/SAIC's access and use of FR information;
 - (b) Ensure that STACC/SAIC personnel have read and signed off on the FR Policy and received the designated training before becoming STACC/SAIC authorized users with access to FR information;
 - (c) Ensure that, within five (5) days of a STACC/SAIC authorized user's transfer, termination, or other separation from the STACC/SAIC, notification is provided to the appropriate entities to revoke that user's ability to access or receive FR information;
 - (d) Maintain a list of all STACC/SAIC authorized users, which is communicated to STACC/SAIC leadership and staff;
 - (e) Conduct audits to ensure compliance with applicable laws, regulations, standards, and policy.
2. STACC/SAIC authorized users are responsible for taking reasonable measures to protect the P/CRCL of individuals, as well as the security and confidentiality of FR data. This includes, but is not limited to:
 - (a) Reading and signing off on the FR Policy and completing the approved training;
 - (b) Following SOPs for documenting information in Memex when the user queries the FR system.
3. The STACC/SAIC Privacy and Compliance Officer will annually review and update the FR Policy and make recommendations for changes in response to changes in applicable law, implementation experience, and the results of audits and inspections.

4. The STACC/SAIC Privacy and Compliance Officer will receive reports regarding alleged errors and violations of the provisions of the FR Policy, will receive and coordinate complaint resolution under the redress provision, and will ensure that P/CRCL protections are implemented through efforts such as training, business process changes, and, where applicable, system designs that incorporate privacy-enhancing technologies.
5. The STACC/SAIC's Operations Commander or Designee or OHS Security Manager or Designee will ensure that enforcement procedures and sanctions outlined in the FR Policy are adequate and enforced.

D. ACQUIRING AND RECEIVING FACE RECOGNITION INFORMATION

1. STACC/SAIC authorized users may directly (e.g., third party vendor/agency contract) or indirectly (e.g., Ohio Law Enforcement Gateway (OHLEG) platform for law enforcement; Business Application Service System (BASS) platform that interfaces with BMV operations) access and perform FR searches for legitimate law enforcement and homeland security purposes as set forth in Section A.3. Such searches may include mug shot images, driver's license photographs, or state identification card images.
2. For the purpose of performing FR searches, STACC/SAIC authorized users may obtain or accept probe images (a face image used by FR software for comparison with the face images contained in a face image repository) only from law enforcement or criminal justice agencies and only for the authorized uses identified in Section A.3.
3. STACC/SAIC authorized users will not perform or request FR searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, national origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law.
4. The STACC/SAIC will contract only with commercial FR companies which provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging FR data comply with applicable local, state, tribal, territorial, and federal laws, regulations, and policies, and that these methods are not based on unfair or deceptive information collection practices.
5. The STACC/SAIC will not directly or indirectly seek, receive, accept, or retain FR information from an individual who, or information provider that, is legally prohibited from obtaining or disclosing the FR information.

E. USE OF FACE RECOGNITION INFORMATION

1. STACC/SAIC authorized users may access, use, and disseminate FR information only for legitimate law enforcement or homeland security purposes as set forth in Section A.3.

2. STACC/SAIC authorized users shall not access, use, or disseminate FR data for:
 - (a) Any purpose that violates the Constitution or laws of the United States;
 - (b) Personal purposes, or non-law enforcement or non-homeland security related purposes;
 - (c) The purpose of prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute;
 - (d) Discriminating, harassing, and/or intimidating any individual or group;
 - (e) Any other access, use, disclosure, or retention that would violate applicable federal or state law or regulation, or departmental policy or SOP.
3. The STACC/SAIC does not connect the FR system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras.

F. SHARING AND DISSEMINATION FR INFORMATION

1. STACC/SAIC authorized users will not do the following with FR information:
 - (a) Sell, publish, exchange, or disclose to commercial or private entities or individuals, except as required by law or to the extent authorized by a department-approved contract with a commercial vendor.
 - (b) Disclose or publish unless required under law and after notification to the originating entity.
 - (c) Disseminate to unauthorized individuals.
2. STACC/SAIC authorized users will not confirm the existence or nonexistence of FR data to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

G. DATA QUALITY ASSURANCE

1. STACC/SAIC authorized users will protect the integrity of original FR data and will not alter, change, or modify it.
2. The STACC/SAIC considers the results, if any, of a FR search to be advisory in nature as an investigative lead only. FR search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.
3. The originating agency is responsible for reviewing the quality and accuracy of FR data and taking reasonable steps to correct or amend any faulty data upon notice from the STACC/SAIC. The STACC/SAIC will, to the extent possible, correct, notate, delete, or refrain from using FR data found to be erroneous or deficient.

H. REDRESS

1. Disclosure

FR information may not be disclosed to the public if it meets one or more exceptions under Ohio public records law, including but not limited to: R.C. §§149.43, 149.433, 1347.01-1347.15, 4501.27, 4507.53, or 5502.03.

Upon satisfactory verification (i.e., fingerprints, driver's license, or other specified identifying information) of his or her identity, an individual may request copies of his/her FR information that has been received by the STACC/SAIC for purposes of challenging its accuracy or completeness by contacting the STACC/SAIC Privacy and Compliance Officer at the following address: Ohio Department of Public Safety, Statewide Terrorism Analysis and Crime Center, ATTN: Privacy and Compliance Officer, 2855 West Dublin-Granville Road, Columbus, Ohio 43235. The STACC/SAIC shall respond within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests. The existence, content, and source of the information **will not be** made available to an individual when:

- (a) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (e.g., R.C. §§109.57, 149.43, 1347.08, 1347.12, 5502.01, 5502.011, 5502.03, 5503.02);
- (b) Disclosure would endanger the health or safety of an individual, organization, or community (e.g., R.C. §§149.433, 1347.12; *Kallstrom v. City of Columbus*, 165 F. Supp.2d 686, S.D. Ohio, 2001; *State ex rel. Plunderbund Media, L.L.C. v. Born*, 141 Ohio St.3d 422 (2014));
- (c) The information is in a criminal intelligence system (28 C.F.R. Part 23);
- (d) The information is protected by state or federal statute (e.g., R.C. §§109.57, 149.43, 149.433, 1347.08, 1347.12, 4501.27, 4507.23, or 5502.03).

2. Complaints and Corrections

If an individual has requested and received FR information about himself/herself and has a complaint or objection regarding the accuracy or completeness of the data, he/she may submit a complaint or request for correction to the STACC/SAIC Privacy and Compliance Officer at the address in this section.

- (a) The STACC/SAIC will, within a reasonable period of time, investigate whether the disputed information is accurate and will notify the individual of the results.
- (b) If the investigation reveals any inaccuracies, the STACC/SAIC will take the following action:
 - (i) If the FR data originated from another agency, the STACC/SAIC will inform that agency of the error and request that the originating agency correct the deficiencies or purge any information that cannot be verified or corrected;
 - (ii) If the STACC/SAIC was the originating agency of such FR data, it will correct the deficiencies or purge any information it cannot verify or correct
- (c) If the investigation reveals that the information is accurate and complete, the STACC/SAIC will decline the individual's request to correct the record (as set

forth in Section I. 2. (b)(i) or (ii)) and inform the individual of the procedure for appealing its decision.

I. SECURITY AND MAINTENANCE

1. The STACC/SAIC will operate in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. FR information accessed by STACC/SAIC authorized users will only be transmitted over secure networks.
2. Access to FR information will be granted only to STACC/SAIC personnel whose positions and job duties require such access and who have successfully completed the requirements in Section B.
3. Usernames or passwords to FR data, if applicable, are not transferable, must not be shared by STACC/SAIC personnel, and must be kept confidential.
4. Queries for FR data by STACC/SAIC authorized users must be logged in such a way that it identifies the user initiating the inquiry. All user access and queries are subject to review and audit by STACC/SAIC leadership.
5. The STACC/SAIC will store FR information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
6. The STACC/SAIC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made as soon as practical and without unreasonable delay following discovery or notification of the access to the information. Such notice shall occur after first notifying the Privacy and Compliance Officer and appropriate agency personnel and subject to the legitimate needs of law enforcement to investigate the release and consistent with any measures necessary to determine the scope of the release and reasonably restore the integrity of the data system.

J. INFORMATION RETENTION AND PURGING

All FR information received and retained by the STACC/SAIC will be kept in accordance with the applicable retention schedule for the record in which such data appears (e.g., FR data within a criminal intelligence record or investigative case file is then considered intelligence or investigative information and the laws, policies, and schedules applicable to that type of information or intelligence govern its use).

K. ACCOUNTABILITY AND ENFORCEMENT

1. Transparency

- (a) The STACC/SAIC will be open with the public in regard to FR information receipt, access, use, dissemination, retention, and purging practices. The FR Policy will be made available upon request and may be accessed as a resource document off the OHS website at <http://homelandsecurity.ohio.gov>.
- (b) The Privacy and Compliance Officer will be responsible for receiving and responding to FR-related inquiries and complaints as specified in Section H.

2. Accountability

- (a) The STACC/SAIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of the FR Policy and applicable law.
- (b) STACC/SAIC personnel shall report errors and suspected or confirmed violations of the FR Policy to the STACC Operations Commander or Designee or OHS Security Manager or Designee.
- (c) The Privacy and Compliance Officer will review the FR Policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or purpose and use of the FR system it accesses.

3. Enforcement

If a STACC/SAIC authorized user is found to be noncompliant with the provisions of the FR Policy regarding the receipt, access, use, dissemination, retention, or purging of FR information, the STACC Operations Commander or Designee or the OHS Security Manager or Designee will:

- (a) Suspend or discontinue the person's access to FR data;
- (b) Suspend, demote, transfer, or terminate the person, as permitted by applicable agency and/or STACC/SAIC policies;
- (c) Apply administrative actions or sanctions as provided by agency rules or policies; and/or
- (d) Refer the matter to the Ohio State Highway Patrol and/or the Federal Bureau of Investigation for criminal prosecution, if necessary, to effectuate the purposes of this policy.

L. TRAINING

- 1. STACC/SAIC authorized users must participate in training programs regarding implementation of and adherence to the FR Policy.
- 2. The STACC/SAIC FR Policy training program will cover:
 - (a) Substance and intent of the provisions of the FR Policy, as well as the P/CRCL protections on the use of the technology and the information received;
 - (b) How to implement the FR Policy in the day-to-day work of the user;
 - (c) Mechanisms for reporting violations of STACC/SAIC FR Policy provisions;
 - (d) The nature and possible penalties for FR Policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Ohio Homeland Security
Statewide Terrorism Analysis & Crime Center



Terrorism Analysis Unit



Standard Operating Procedures
Facial Recognition Request

Updated July 2018

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

The STACC receives Facial Recognition Requests (FRRs) from the National Fusion Center Network via the Homeland Security Information Network (HSIN) referenced as MSFR's (Multi State Facial Recognition) requests. The results of a submission are for lead purposes only, and further confirmation as to the identity of the submission shall be the sole responsibility of the requester. In order to ensure STACC personnel are complying with the rules set forth by OHLEG the following steps will be taken when processing OHLEG facial recognition requests:

1. All Ohio Driver's licenses, ID photos, and all other photos will remain in the custody of the originating agency or OHLEG but will not otherwise be transferred to any other entity
2. Images entered into the OHLEG facial recognition system will not be released to anyone other than the law enforcement personnel who made the request and only in conjunction with an authorized criminal investigation.
3. OHLEG facial recognition requests can only be submitted in conjunction with an official law enforcement investigation. Analysts must keep a log with an entry, showing the case number/request for assistance, Originating Agency Identifier (ORI) number/Case Number and type of criminal investigation being conducted, for every use of the facial recognition tool.
4. An STACC supervisor must approve any dissemination of facial recognition images or search results beyond the agency or officer who originally requested the information.

The facial recognition log will be stored in the "20XX STACC Progress Tracker" on the Law Enforcement Portion of the P: drive in the common folder for that specific year. Analysts must ensure they log all facial recognition request in the tracker. Memex entries for facial recognition requests should include a reference to the facial recognition logged in the tracker.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

INTER-OFFICE COMMUNICATION

Date September 23, 2014

File 3-POL



To OSP-HUB Intelligence Unit Personnel Attention

From Lieutenant M. K. Hasson, Intelligence Unit Commander

Subject OHLEG Facial Recognition Inquires

The OSP-Hub Intelligence Unit has recently become the contact point for the Division's OHLEG facial recognition inquiries. In order to ensure Intelligence Unit personnel are complying with the rules set forth by OHLEG the following steps will be taken when processing OHLEG facial recognition requests:

- 1) Images entered into the OHLEG facial recognition system will not be released to anyone other than the law enforcement personnel who made the request and only in conjunction with an authorized criminal investigation.
- 2) OHLEG facial recognition requests can only be submitted in conjunction with an official law enforcement investigation. Analysts must keep a log with an entry, showing the **case number** and type of criminal investigation being conducted, for every use of the facial recognition tool.
- 3) An Intelligence Unit supervisor must approve any dissemination of facial recognition images or search results beyond the agency or officer who originally requested the information.

The facial recognition log will be stored in the "20XX OHLEG " on the for that specific year. Analysts must complete the log prior to completing facial recognition requests. Memex entries for facial recognition requests should include a reference to the facial recognition log being completed.

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

Introduction

The Ohio Attorney General's (AGO) Bureau of Criminal Investigation (BCI), is responsible for the operation of the Ohio Law Enforcement Gateway (OHLEG). As an information resource, OHLEG is a strategic asset of the AGO and must be treated and managed as a valuable resource. This policy documents expectations for appropriate use of OHLEG. The OHLEG Data Security Use Policy in conjunction with the OHLEG Rules and Regulations are established to achieve the following:

1. To establish acceptable practices regarding the use of information resources.
2. To ensure compliance with applicable local, state and federal law and other rules and regulations regarding the management of information resources.
3. To educate individuals who use OHLEG regarding applicable laws, rules, and regulations.
4. This OHLEG Data Security Use Policy contains the following four policy components: (1) Use Management Requirements and Ownership; (2) Use Requirements; (3) Agency Responsibilities; and (4) Enforcement, Auditing, Reporting and Monitoring. Together, these directives form the foundation of the BCI OHLEG Acceptable Use Program.

Roles & Responsibilities

BCI OHLEG management in cooperation with AGO ITS will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

BCI OHLEG management in cooperation with AGO ITS is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.

BCI OHLEG management and OHLEG administration, in cooperation with AGO ITS, are required to train users on policy and document issues with Policy compliance.

All OHLEG users and Agency management are required to read and acknowledge this policy.

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

Policy Directives

Use Management Requirements

The AGO shall establish formal Standards and Processes to support the ongoing development and maintenance of the BCI OHLEG Data Security Policy.

BCI OHLEG management and AGO management commit to the ongoing training and education of AGO staff responsible for the administration, maintenance and use of BCI OHLEG information resources. At a minimum, skills to be included or advanced include OHLEG administrator training and Security Awareness training.

Security Events that could pose a risk to the data or operation of BCI OHLEG shall be reported to the BCI OHLEG Support Center. Additional Reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.

Ownership

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the AGO are the property of the AGO and use of such information is neither personal nor private. AGO management reserves the right to monitor and/or log all use of AGO information resources with or without prior notice.

Use Requirements

1. Users shall report any known weaknesses in computer security to the appropriate agency security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
2. Users shall report any incidents of possible misuse or violation of this OHLEG Data Security Use Policy to the BCI OHLEG Support Center.
3. Users shall not attempt to access any data, documents, email correspondence, and/or programs contained on BCI OHLEG information resources for which they do not have authorization.
4. Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
5. Users shall not make unauthorized copies of BCI OHLEG owned software.

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

6. Users shall not use shareware or freeware software without the appropriate management approval from their respective agency. Any such software must not permit access to any BCI OHLEG data or resources.
7. Users shall not engage in activity that may degrade the performance of BCI OHLEG information resources; deprive an authorized user access to BCI OHLEG information resources; obtain extra resources beyond those allocated; or circumvent BCI OHLEG information resources security measures.
8. Users shall not download, install or run security programs or utilities such as, but not limited to password cracking programs, packet sniffers, or port scanners that attempt to reveal or exploit weaknesses in the security of a BCI OHLEG information resource unless approved by AGO ITS Security.
9. All users shall read and adhere to all BCI OHLEG information assurance directives and policies posted on OHLEG.
10. All users shall address any questions regarding policy, responsibilities and duties to the BCI OHLEG Support Center.
11. All users shall complete annual Security Awareness training or provide BCI OHLEG administrators with adequate documentation of the completion of their employing agencies' security awareness training. Note that the AGO may require additional security awareness training and will provide training if necessary.
12. All users shall immediately report known or suspected security incidents or improper use of BCI OHLEG, regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information, to the BCI OHLEG Support Center.
13. Users shall operate systems and technology only in a secure environment and when not in use keep them secured to ensure that unauthorized access does not occur.
14. Users shall read and acknowledge all login information and communications concerning the use and access of OHLEG.
15. Users shall ensure that all devices accessing BCI OHLEG information resources are secure and free from malicious code.
16. Users shall use strong passwords on all devices used to access BCI OHLEG information resources. (strong passwords are defined as; 8 characters that are a combination of upper case letters, lower case letters, numbers and special characters)

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

17. Users shall use unique accounts and passwords for all systems and never share accounts or passwords with any other person or use any other person's accounts and passwords to access any BCI OHLEG information resource.
18. All users acknowledge that it is their responsibility to protect the information contained in BCI OHLEG to the best of their ability.
19. Users shall use screen locks with password protection on all devices used to access BCI OHLEG information resources.
20. Users shall never make unauthorized copies of any BCI OHLEG data or applications.
21. All devices used to access BCI OHLEG information resources shall have up to date antivirus software running at all times, employ the use of firewalls and have all security related operating system patches applied and supported internet browser versions installed and updated with all vendor security patches. BCI OHLEG and / or AGO ITS administration reserves the right to deny access to any device that does not comply.
22. Any attempt to circumvent any policy, intentional or unintentional may result in the loss of access to BCI OHLEG resources and could result in possible criminal charges.
23. All users acknowledge that they are solely responsible for all activities performed under their account.
24. All users acknowledge that access to OHLEG is limited to use for official law enforcement/administration of criminal justice purposes only. OHLEG access is NOT to be used for personal use or gain.

Agency Responsibilities

Each agency is responsible for the activities of users assigned to their agency. Agency management shall acknowledge the OHLEG Data Security Use Policy for each person they assign to their respective agencies and are required to acknowledge Agency Responsibilities. BCI OHLEG information resources provide the ability for agency management to identify those individuals electronically.

1. Agency management shall provide to BCI OHLEG management notification of any user status change.
2. Agency shall take reasonable measures to ensure that the agency network is secure and free from malicious code.
3. Agency has a documented Security Policy that includes but is not limited to; password controls, user account activation and deactivation process, Incident Process and Procedure and requirements for end point and perimeter protection,

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

this includes but is not limited to; Antivirus Software, Antimalware software, Disk Encryption, Personal Computer Firewalls, Personal Computer Intrusion Detection Software and Intrusion Prevention Software..

4. Agency management must provide documentation that all users have received security awareness training.
5. Agency management acknowledges that BCI OHLEG management reserves the right to deny the agency access to BCI OHLEG information resources if an event is noted that could potentially put the BCI OHLEG information resources or data at risk.
6. Agency management understands that all access to BCI OHLEG information resources are monitored, logged and audited.
7. All agency users are required to complete a BCI OHLEG request for access form to obtain an account in BCI OHLEG.
8. Agency shall consent to review of security controls and provide adequate documentation upon request.
9. Agency management shall ensure that any computer and/or network used to assess BCI OHLEG information resources does not contain security tools that could be directed to BCI OHLEG information resources. Security tools are those used to perform analysis of vulnerabilities in computer systems as well as simulate network or computer attacks that could be detrimental to BCI OHLEG.
10. Agency management shall consent to requests for review of any equipment used to access AGO Information Resources.

Enforcement, Auditing, Reporting, Monitoring

Violation of this policy may result in disciplinary action that may include termination of access to BCI OHLEG information resources. Termination of rights for BCI OHLEG information resources may also be applied to other AGO information resources services and/or products. Additionally, individuals may be subject to civil and/or criminal prosecution.

BCI OHLEG administration is responsible for the periodic auditing and reporting of compliance with this policy.

Any user may, at any time, anonymously report policy violations via AGO provided resources. Anyone that wishes to report a violation should contact the BCI OHLEG Support center.

All users shall agree that all access to data, software, media, and hardware is strictly monitored and access can be revoked if determined that inappropriate use has been identified.

Bureau Of Criminal Investigations Ohio Law Enforcement Gateway Data Security Use Policy

All applications and data are on a need to know basis. Any unauthorized access, use or dissemination of any data is considered a breach of security and could result in revocation of use rights and / or civil and criminal charges.

Control and Maintenance

AGO Policy will be reviewed and revised in accordance with parameters established in the AGO Security Policy.

User Acknowledgment

I acknowledge that I have read and understand the above listed policy. I acknowledge that I am responsible for reading and understanding the OHLEG Rules and Regulations. I also state that I will adhere to these directives and that failure to do so may constitute a security violation resulting in denial of access to BCI OHLEG information resources as well as other products and services provided by the AGO. I also understand that violation of this policy will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate

PrintedName: _____ Date: _____

Signature: _____ ORI #: _____

Agency
Name: _____

Agency Acknowledgment

I acknowledge that I have read and understand the above listed policy. I acknowledge that I am responsible for reading and understanding the OHLEG Rules and Regulations. I also state that I am responsible for the users that are assigned to my charge and will adhere to these directives and that failure to do so may constitute a security violation resulting in denial of access to BCI OHLEG information resources as well as other products and services provided by the AGO. I also understand that violation of this policy will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate

PrintedName: _____ Date: _____

Title: _____

Signature: _____ ORI #: _____

OHLEG

OHIO LAW ENFORCEMENT GATEWAY



Rules and Regulations

Effective July 1, 2016



Tom Stickrath
Superintendent



MIKE DeWINE
★ OHIO ATTORNEY GENERAL ★

Contents

Contact Information	3
Terms and Definitions	3
Acronym List.....	8
Introduction	9
Access	10
1.0 OHLEG Agency/User Agreements	10
1.1 Access Restrictions	10
1.2 Access Control Criteria.....	11
1.3 System Use Notification	11
1.4 Personnel Security.....	12
1.5 OHLEG Access Procedure	13
1.6 New Agency OHLEG Application	14
1.7 Out-of-State Agency OHLEG Application	14
1.8 Security Awareness Training.....	16
1.9 All Personnel	16
1.10 OHLEG Practice and Test Inquiries.....	17
1.11 Facial Recognition	17
Management	19
2.0 Participating Agency Chief Executive Responsibility	19
2.1 User Account Management.....	19
2.2 OHLEG Agency Approver	20
2.3 OHLEG Agency Coordinator.....	20
2.4 Personnel Termination.....	21
2.5 Personnel Action.....	21
2.6 OHLEG Sanctions	21
2.7 Agency Sanctions.....	22
Quality Assurance	22
3.0 Monitoring, Analysis, and Reporting	22
3.1 Special Security Inquiries and Audits	23

3.2	Audit Log Retention	23
3.3	Agency Audit Requests.....	23
3.4	Reporting	24
	Data Security	24
4.0	Criminal Justice Information (CJI)	24
4.1	Criminal History Record Information (CHRI)	25
4.2	Personally Identifiable Information (PII)	25
4.3	Dissemination.....	26
4.4	Dissemination of CJI Related to Discovery Motion.....	26
4.5	CHRI Storage	26
4.6	Passwords	27
4.7	Physical Protection.....	27
4.8	Controlled Area	28
4.9	Personally Owned Information Systems.....	28
4.10	Publicly Accessible Computers.....	28
4.11	Mobile Technologies	28
4.12	Cellular Risk Mitigations.....	29
4.13	Media Protection	29
4.14	Electronic Media Sanitization and Disposal.....	30
4.15	Disposal of Physical Media.....	30
	Technical Compliance	30
5.0	Device and Resource Protection Guidelines	30
5.1	Data Security Threat Incident Response.....	32
	Appendix A: OHLEG Practice and Test Inquiries	33
	Appendix B: Model OHLEG Policy	34
	Appendix C: Referenced Ohio Revised Code.....	38

Contact Information

OHLEG Support:

Main Phone: (866) 406-4534

Email: OHLEGSupport@OhioAttorneyGeneral.gov

BCI Radio Room:

Main Phone: (740) 845-2224

OHLEG Quality Assurance:

Email: OHLEGQualityAssurance@OhioAttorneyGeneral.gov

Terms and Definitions

Access to Criminal Justice Information - The physical or logical (electronic) ability, right or privilege to view, modify, or make use of Criminal Justice Information (CJI).

Administration of Criminal Justice - The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

AGO IT - The information technology section of the Ohio Attorney General's Office.

Authorized Use - The act of using OHLEG in a manner that is consistent with OHLEG security policies, Ohio Revised Code, and with the criminal justice purposes for which the user was granted OHLEG access.

Biographic Data - Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data - When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case/Incident History - All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regard to CJI, it is the information about the history of criminal incidents.

Criminal History Record Information (CHRI) - A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) - The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Information (CJI) - Criminal Justice Information is the abstract term used to refer to all of the OHLEG-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data.

Criminal Justice Purpose - The motivating reason behind a user action, derived from the user's work related duties or needs in furtherance of the administration of criminal justice.

Department of Justice (DOJ) - The department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just

punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Dissemination - The transmission/distribution of CJI to another person or agency.

Encrypted (data) - Computer data that is converted into an incomprehensible form through the use of a key. Only a holder of a matching key can restore the data to its original form.

Facial Recognition (FR) - An OHLEG attribute that allows unidentified photos from a police investigation to be searched by facial feature comparison against a database of known person's photos.

Information System - A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Law Enforcement Activity (as used in Section 2.6 Facial Recognition) - An activity, carried out by duly authorized law enforcement personnel pursuant to their official duties, that is consistent with law and is grounded in a reasonable belief based on a totality of circumstances that the use of facial recognition may result in an investigative lead with respect to a specific criminal matter; reduce an imminent threat to health or safety; or assist in the identification of someone who is not able to identify him or herself.

Law Enforcement Agency - A police department, the office of a sheriff, the state highway patrol, a county prosecuting attorney, or a federal, state, or local governmental body that enforces criminal laws and has employees who have a statutory power of arrest.

Logical Access - In computer security, being able to interact with data through access control procedures such as identification, authentication and authorization.

Misuse - Any utilization of OHLEG that is not directly related to the administration of criminal justice, or that is inconsistent with OHLEG security policies, Ohio Revised Code, Ohio Administrative Code, or the criminal justice purposes for which the user was granted OHLEG access. This includes, but is not limited to, uses motivated by the personal interest of the user or for the user's commercial benefit, as determined by the Director of OHLEG.

OHLEG Agency Approver (Approver) - An OHLEG user designated by the agency CEO to approve OHLEG Access Applications.

OHLEG Agency Coordinator (OAC) - An OHLEG user who will serve as the point of contact at each OHLEG Participating Agency with specific duties and responsibilities for administering OHLEG security policies in support of the agency CEO.

OHLEG Agency Identifier (OAI) - An alphanumeric agency identifier which could be either a CJIS-issued ORI or an OHLEG-issued equivalent for agencies unable to obtain an ORI.

OHLEG Agency/User Agreement - A terms-of-service acknowledgment that must be signed prior to obtaining agency or individual user OHLEG access. This acknowledgment must be signed on behalf of the agency and also by each individual user.

OHLEG Director - Senior staff member of BCI administration responsible for oversight and administration of all OHLEG-related functions in support of the Superintendent of BCI.

OHLEG Executive Management - The Superintendent of the Ohio Bureau of Criminal Investigation, the Assistant Superintendent of BCI, and the OHLEG Director.

OHLEG Participating Agency (Agency) - A criminal justice agency (CJA) that has been granted access to OHLEG.

OHLEG Security Policies - The term used to encompass all forms of guidance or directives used by OHLEG to control and direct OHLEG agency and user access, usage, behavior and conduct. This term includes but is not limited to: OHLEG Rules and Regulations, OHLEG site notifications and acknowledgements, and OHLEG directives, messages, and security training videos.

OHLEG User - An individual authorized to access OHLEG, who has been appropriately vetted through a national fingerprint-based record check and has been granted access to CJI data.

Personal Use - Use of OHLEG, outside of official business for the agency.

Personally Identifiable Information (PII) - Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name and date of birth, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Probationary Access (Probation) - A sanction which requires a period of supervised OHLEG usage before being restored to full OHLEG access.

Property Data - Information about vehicles and property associated with a crime.

Task Force - A group initiative involving the structured, organized, collaborative effort of multiple law enforcement agencies that targets a particular criminal activity, often in a particular geographical area.

Secondary Dissemination - The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. These include but are not limited to: attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Validation - An action performed by either a participating agency or OHLEG auditors or administration to verify that OHLEG user authorizations, access, training and other security policy requirements are accurate, appropriate and up to date.

Acronym List

AGO	Attorney General's Office
BCI	Ohio Bureau of Criminal Investigation
CEO	Chief Executive Officer
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
LEADS	Law Enforcement Automated Data System
OAC	OHLEG Agency Coordinator
OAI	OHLEG Agency Identifier
OHLEG	Ohio Law Enforcement Gateway
ORC	Ohio Revised Code
ORI	Originating Agency Identifier
PII	Personally Identifiable Information
QAS	Quality Assurance Specialists

Introduction

The Ohio Attorney General created the Ohio Law Enforcement Gateway (OHLEG) to allow practitioners to have timely and secure access to criminal justice data. The OHLEG Rules and Regulations were created for criminal justice agencies using OHLEG to ensure that the sources, transmission, storage, and generation of Criminal Justice Information (CJI) are protected.

The OHLEG Rules and Regulations apply to every OHLEG user as well as non-user members of Criminal Justice Agencies (CJA) who handle Criminal Justice Information obtained through OHLEG in the course of their duties.

The Rules and Regulations are designed to allow sufficient flexibility for participating agencies to structure their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this document.

The OHLEG staff developed the first version of the OHLEG Rules in April 2005. The rules were expanded in June 2014 to address the privacy concerns of Ohio citizens related to newly developed OHLEG software applications. This updated version of OHLEG Rules refines the expanded rules and incorporates the OHLEG Data Security Use Policy into the Rules and Regulations document.

All OHLEG users are required to read and abide by the OHLEG Rules and Regulations. OHLEG quality assurance provides assistance with agency audits and investigations and works to ensure compliance with rules and regulations. OHLEG support works tirelessly to keep users' account access functioning and accessible. OHLEG administration's goal is to keep this invaluable tool available for use by criminal justice agencies working to protect the citizens of Ohio while respecting the privacy rights of those same citizens. Assisting in this effort OHLEG would like to acknowledge the contribution and assistance of the OHLEG Advisory and Steering Committees in the development and production of this rules and regulations document. Their valued counsel contributes significantly toward the achievement of this goal.

Access

1.0 OHLEG Agency/User Agreements

Any CJA receiving access to OHLEG must sign the OHLEG Agency/User Agreement. The agency CEO will sign an agreement on behalf of the agency. By signing this agreement, the agency acknowledges that it is responsible for enforcing and adhering to all OHLEG Security Policies, as well as accepting responsibility for all users gaining access through that agency.

Additionally, each individual user must also sign an OHLEG Agency/User agreement. The individual user agreements will be kept on file at the agency, where they will be subject to inspection by OHLEG Quality Assurance. By signing this agreement, all users acknowledge they are responsible for reading and understanding all OHLEG Security Policies and will be held accountable for violating them. All users also acknowledge that access to OHLEG is limited to use for criminal justice purposes only. OHLEG access is NOT to be used for personal use.

The OHLEG Agency/User Agreement is available on the OHLEG website.

The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI. BCI's grant of access to OHLEG confers no process or other rights in maintaining such access.

1.1 Access Restrictions

Criminal justice professionals who work for a law enforcement agency (e.g., police officers and sheriff's deputies) require a greater degree of OHLEG access than those who work for non-law enforcement agencies (e.g., court employees). For this reason OHLEG law enforcement users will be given access to a wider range of OHLEG attributes than will non-law enforcement users.

The CEO of each agency bears the primary responsibility for determining and enforcing access restrictions. OHLEG users are permitted only to access OHLEG attributes that are directly related to their job responsibilities. Access to individual attributes shall be based on the agency to which the user is assigned at the time of use. OHLEG users who participate through multiple agencies shall only log on to OHLEG using the OAI number for the

agency for which they are working at the time of access. The attributes are to be determined by the CEO or designee at the time of the user's request for access and should be reviewed when job assignments or responsibilities change. Task Force members wishing to obtain a separate OHLEG account as part of their Task Force duties should contact the BCI/OHLEG Support Center.

The nexus between an account holder's job assignment and OHLEG access is subject to review and validation during OHLEG Quality Assurance visits. Furthermore, users shall not attempt to access any data, documents, email correspondence, and/or programs contained on BCI/OHLEG information resources for which they do not have authorization.

1.2 Access Control Criteria

Agencies should consider the following when establishing rules that control access to CJI:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
4. Time-of-day and day-of-week/month restrictions.

1.3 System Use Notification

OHLEG will display an approved system use notification message, before granting access, informing potential users of various usage and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. Unauthorized use of the system is prohibited and a violation of criminal law.
3. System usage is subject to monitoring, recording, and auditing.

4. Use of the system indicates consent to monitoring and recording. The system includes all data, software, media, and hardware.
5. The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI. BCI's grant of access to OHLEG confers upon the user no process or other rights in maintaining such access.

The system use notification message and any communications must be acknowledged before the user can gain access to the system.

1.4 Personnel Security

Having proper security measures against the insider threat is a critical component of the OHLEG security policies. This section's security terms and requirements apply to all personnel who have access to OHLEG including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI. Access to OHLEG is a privilege and not a right.

The minimum screening requirements for individuals requiring access to CJI are as follows:

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to OHLEG or CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to OHLEG.
2. The agency CEO shall specify the agency process for requesting OHLEG access.
3. If a felony conviction of any kind exists, the agency CEO shall deny access to OHLEG. However, the CEO may ask for a review by the OHLEG Director in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

4. If the person has a non-felony conviction or any arrest history without conviction, access to CJI shall not be granted until the agency CEO reviews the matter to determine if access is appropriate.
5. If the person has an arrest history that includes any theft, domestic violence, menacing, or stalking offense; telecommunications harassment; or any misuse of OHLEG, LEADS, or misuse of any law enforcement restricted database or information, the CEO shall deny access. The CEO may ask for a review by the OHLEG Director as indicated in #3 above.
6. If the person appears to be a fugitive the person will be denied access to OHLEG.
7. If the person already has access to CJI and is subsequently arrested and/or convicted of a crime, access to OHLEG shall be terminated. If the crime is a non-felony, OHLEG access may be reinstated following a review by the agency CEO consistent with #4 and #5 above.
8. If the agency CEO, OAC, or OHLEG Director determines that access to OHLEG by an applicant/user would not be in the public interest, access shall be denied/removed. If access is denied/removed under this section, the agency shall notify the BCI/OHLEG Support Center in writing.
9. BCI/OHLEG's determination as to an OHLEG user's status is independent of, and unrelated to, his/her employment situation with their agency. BCI will not make any determination about an OHLEG user's job status, a matter over which BCI exercises no authority or discretion.

1.5 OHLEG Access Procedure

No OHLEG user shall attempt to gain access to OHLEG or any OHLEG attribute beyond the specific access limits established and authorized by his or her employing agency.

1. Requests for OHLEG access will be made via the OHLEG Online Account Application attribute, which is available on the homepage of any current OHLEG user.
2. On each new user application, the Approver is required to certify that the basic training security video for a new OHLEG user has been viewed by

the applicant. The Approver must also certify that the OHLEG Agency/User Agreement has been signed by the user.

3. The new applicant must then physically enter his or her personal information in the appropriate sections on the online application.
4. The Approver will select from a checklist which available OHLEG attributes are approved for each applicant.
5. The Approver shall submit applications electronically to OHLEG administration for further processing and activation.
6. The Facial Recognition attribute will require specific authorization by the CEO and justification for each user indicating the investigative or other area of responsibility requiring such access.
7. Non-law enforcement agencies generally will not have access to the Facial Recognition attribute. Any non-law enforcement agency believing it has an exceptional need for access to the Facial Recognition attribute may apply to the Superintendent of BCI for Facial Recognition access.

1.6 New Agency OHLEG Application

All agencies new to OHLEG must complete a New Agency Application form. Please contact the BCI/OHLEG Support Center to request this form.

1.7 Out-of-State Agency OHLEG Application

OHLEG allows out-of-state law enforcement agencies to have OHLEG access based on specific need. This need may be indicated by an Ohio border jurisdiction or an Ohio related investigation. Such access serves the mutual interest of law enforcement agencies outside of Ohio and Ohio criminal justice. Out-of-state law enforcement agencies may apply for OHLEG access as an OHLEG Participating Agency.

Procedure:

1. The out-of-state law enforcement agency must apply for agency status by filling out the OHLEG Out-of-State Agency Application, which can be found on OHLEG or obtained from the BCI/OHLEG Support Center.
2. The application must state the specific criminal justice purpose OHLEG access will meet for the applying agency and how OHLEG access will be used if granted.
3. If granted, only OHLEG attributes related to the specific needs of the agency will be authorized.
4. OHLEG access granted to any out-of-state law enforcement agency will be for a limited specific time period not to exceed one year. Out-of-state access is renewable through the application process on a yearly basis.
5. The applying agency must acknowledge its understanding that misuse of OHLEG constitutes a criminal violation of Ohio law and that such cases will be turned over to an Ohio county prosecuting attorney for prosecution under the applicable Ohio statute.
6. Out-of-state law enforcement agencies will be required to adhere to OHLEG security policies including CEO supervision and audit compliance.
7. Out-of-state law enforcement agencies as a general rule will not have access to the Facial Recognition attribute. Any out-of-state law enforcement agency believing it has an exceptional need for access to the Facial Recognition attribute may apply to the Superintendent of BCI for Facial Recognition access.
8. Out-of-state, non-law enforcement criminal justice agencies will not be granted OHLEG access without the express written authorization of the Superintendent of BCI.

1.8 Security Awareness Training

An OHLEG Security Training Video will be made available online. Viewing of the OHLEG Security Awareness Training video shall be required before OHLEG access and initial assignment credentials are issued. Security awareness training will be required every two years thereafter for all personnel with access to OHLEG. This biennial training can be accomplished by watching the current OHLEG Security Training video or by completing agency security awareness training that meets the requirements in Section 1.9. The agency shall document user training and provide such documentation upon request. Note that the AGO/BCI/OHLEG may require additional security awareness training and will provide training if necessary.

1.9 All Personnel

At a minimum, the following topics shall be addressed as security awareness training for all authorized personnel with access to OHLEG:

1. Rules that describe responsibilities and expected behavior with regard to OHLEG system usage.
2. Implications of noncompliance.
3. Incident response (points of contact; individual actions).
4. Media protection.
5. Password usage and management – including creation, frequency of changes, and protection.
6. Protection from viruses, worms, Trojan horses, and other malicious code.
7. Unknown e-mail/attachments.
8. Web usage – allowed versus prohibited; monitoring of user activity.
9. Spam.
10. Social engineering.
11. Physical Security – increases in risks to systems and data.
12. Handheld device security issues – address both physical and wireless security issues.

13. Laptop security – address both physical and information security issues.
14. Personally owned equipment and software – state whether allowed or not (e.g., copyrights).
15. Access control issues – address least privilege and separation of duties.
16. Individual accountability – explain what this means in the agency.
17. Use of acknowledgement statements – passwords, access to systems and data, and personal use.
18. Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
19. Protecting information subject to confidentiality concerns – in systems, archived, on backup media, and until destroyed.
20. Dissemination and destruction.

1.10 OHLEG Practice and Test Inquiries

In order for OHLEG users to familiarize themselves with the OHLEG Search Engine (SE) or to test system functionality, practice/test inquiries have been provided and posted onto OHLEG and are attached in Appendix A of this document. **OHLEG USERS ARE NOT ALLOWED TO RUN SEARCHES ON THEMSELVES OR FAMILY MEMBERS**—such searches will trigger an audit by OHLEG Quality Assurance.

1.11 Facial Recognition

Facial recognition technology is an investigative tool. Law enforcement should use it to generate an investigative lead in an active criminal matter in order to solve or prevent crime, to reduce an imminent threat to health or safety, or to identify someone who is not able to identify himself or herself. Law enforcement may not employ this technology to conduct dragnet screening of individuals, nor should it use it to facilitate mass surveillance of places, groups, or activities unless doing so furthers an official law enforcement activity. For example, it would not be appropriate for law enforcement to use facial recognition technology to conduct surveillance of persons or groups based solely on their religious, political, or other

constitutionally protected activities or affiliations unless doing so furthers an official law enforcement activity.

The use of the Facial Recognition attribute as an investigative tool will fall under the same rules as those applied to OHLEG CJI with the addition of the following:

1. All Ohio drivers' licenses, ID photos, and all other photos will remain in the custody and control of the originating agency or OHLEG but will not be otherwise transferred to any other entity.
2. Images received in a request or submission will not be stored as enrolled images within the Facial Recognition system. A thumbnail photo will be archived for audit purposes, but the photo will not be enrolled in the database and will not be searchable.
3. Images enrolled in the Facial Recognition system will not be released to anyone other than law enforcement personnel and only in conjunction with an authorized criminal investigation.
4. Facial Recognition technology may only be used for an official law enforcement activity. For the purposes of this section, an "official law enforcement activity" shall mean an activity, carried out by duly authorized law enforcement personnel pursuant to their official duties, that is consistent with law and is grounded in a reasonable belief based on a totality of circumstances that the use of facial recognition may:
 - a. Result in an investigative lead with respect to a specific criminal matter;
 - b. Reduce an imminent threat to health or safety;
 - c. Assist in the identification of someone who is not able to identify him or herself.
5. Agencies must keep a log with an entry, showing the date, name, case number, and the type of criminal investigation being conducted, for every use of the Facial Recognition attribute.

6. All Facial Recognition requests and any results of the inquiry will be maintained by OHLEG in accordance with appropriate current OHLEG document maintenance and destruction policies.
7. An agency supervisor must approve any dissemination of Facial Recognition images or search results beyond the originating agency.
8. Disseminations to the press will occur only with OHLEG management and requesting agency authorization.

Management

2.0 Participating Agency (Agency) Chief Executive Responsibility

All OHLEG Participating Agencies are responsible for establishing and administering an OHLEG security program throughout the agency's user community. The Chief Executive Officer (CEO) of each agency is responsible for that agency's adherence to OHLEG security policies. That responsibility includes accountability for individual OHLEG account holders within the CEO's agency. The agency CEO shall appoint an OHLEG Agency Approver and Coordinator. The agency CEO may choose to fill either or both roles him or herself. The CEO, OAC, and Approver will be given access to the OHLEG Roster attribute through which they can manage user account access. The agency may impose more stringent protection measures than those outlined in the OHLEG security policies. Such measures shall be documented and kept current.

2.1 User Account Management

The agency shall manage OHLEG accounts, including applications, training, modifying and reviewing accounts, and validating rosters.

The agency shall grant continued access to the information system based on:

1. Valid need-to-know that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

2.2 OHLEG Agency Approver (Approver)

The Approver is an individual located within the agency responsible for approving OHLEG Access Applications. They are unable to approve Facial Recognition requests, which with limited exceptions must be approved by the agency CEO.

2.3 OHLEG Agency Coordinator (OAC)

The OAC is an individual located within the agency who serves as the main contact person for OHLEG and is responsible for the administration of the OHLEG network for the agency. The agency CEO—through the OAC—shall:

1. Validate the agency OHLEG roster every 90 days. This validation process requires the OAC to confirm that all users listed on the roster are current employees and authorized OHLEG users.
2. Set, maintain, and enforce standards for the selection, supervision, and separation of personnel who have access to OHLEG.
3. Oversee by all appropriate means the adherence by the agency and its users to all OHLEG security policies.
4. Document technical compliance with OHLEG security policies with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the agency's user community.
5. Establish a data security threat incident response and reporting procedure to discover, investigate, document, and report to the agency CEO and OHLEG, incidents that endanger the security or integrity of CJI.
6. Ensure that personnel security screening procedures are being followed as stated in these regulations.
7. Ensure that the approved and appropriate security measures are in place and working as expected.
8. Report data security threat incidents as outlined in Section 5.1.

2.4 Personnel Termination

The agency, upon termination of an individual's employment, shall immediately remove the individual's access to OHLEG through OHLEG Roster or by notifying the BCI/OHLEG Support Center. If the termination is related to OHLEG misuse, the agency CEO or OAC shall notify the BCI/OHLEG Support Center. If the termination is related to other misconduct, the CEO or OAC should consider requesting the user's audit log from OHLEG so the agency can determine whether OHLEG misuse may also have occurred.

2.5 Personnel Action

The agency shall review OHLEG access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing accounts and changing system access authorizations. The agency is also responsible to notify the BCI/OHLEG Support Center and submit new designations whenever there is a personnel change affecting the OHLEG roles of agency CEO, OAC, and/or Approver.

If an OHLEG user is removed from full active duty as a result of a personnel action, including but not limited to, suspension, administrative leave, or disciplinary action, the OAC will initiate an Administrative Review to determine if the user should have access during said removal.

2.6 OHLEG Sanctions

The law enforcement data maintained by BCI on the OHLEG site is provided at, and subject to, the discretion of BCI. BCI's grant of access to OHLEG does not confer upon the agency or its users any process or other rights in maintaining such access. Termination of rights for BCI/OHLEG information resources may also be applied to other AGO information resources services and/or products.

OHLEG sanctions for violations of OHLEG security policies may include any of the following disciplinary actions:

1. Criminal prosecution.
2. Permanent termination of user or agency access.

3. Suspension of user or agency access.
4. Probationary user or agency access.
5. Restricted user or agency access.
6. Mandatory user or agency re-training.

2.7 Agency Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established OHLEG security policies. See Section 3.4 for additional rules governing OHLEG misuse.

Agency sanctions for user misuse may also include the following:

1. Termination of employment.
2. Unpaid suspension of employment.
3. Reprimand.
4. Training or re-training.
5. Performance improvement plan.

Quality Assurance

3.0 Monitoring, Analysis, and Reporting

Electronic files created, sent, and received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the AGO are the property of the AGO and use of such information is neither personal nor private.

OHLEG Access is to be used for criminal justice purposes only. Personal use is strictly forbidden.

OHLEG shall employ Quality Assurance Specialists (QAS) to perform audits to ensure compliance with OHLEG security policies including those applying to both agencies and OHLEG users. OHLEG QAS shall visit agencies to perform audits to ensure this compliance. Random audits shall also be conducted as a matter of course and shall not require a complaint, alleged security violation, or other justification.

OHLEG QAS shall routinely review and analyze agency audit records for suspicious activity or indications of misuse. OHLEG QAS will assist in the investigation of suspected violations and report findings to the appropriate officials.

3.1 Special Security Inquiries and Audits

All agencies having access to OHLEG shall permit an OHLEG Quality Assurance inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the OHLEG Director. All results of the inquiry and audit shall be reported to the agency CEO and OHLEG Director with appropriate recommendations.

3.2 Audit Log Retention

All log records of OHLEG usage kept by the agency, including but not limited to Facial Recognition inquiries and CHRI dissemination logs, are subject to audit at any time. These logs shall be maintained for a minimum period of eight years or a period equal to the agency's internal record retention policy – whichever is greater.

3.3 Agency Audit Requests

An agency may request an audit of an agency employee's OHLEG usage. This audit may be requested as part of an investigation conducted by the agency or as a routine part of agency initiated monitoring. The audit must be requested by either the agency CEO or OAC.

A law enforcement agency, with proper jurisdiction, may find it necessary to conduct a criminal investigation of a user employed by an OHLEG Participating Agency. In such circumstances, the investigating agency may request an OHLEG audit of the subject under investigation. A request for an OHLEG audit of another agency's user must come from the investigating

agency CEO on department letterhead and indicate it is requested as part of a criminal investigation.

OHLEG audit requests may be requested via email at OHLEGQualityAssurance@OhioAttorneyGeneral.gov.

Upon completion of any investigation of OHLEG misuse, the law enforcement agency will forward a copy of the full investigative report to OHLEG for administrative review.

3.4 Reporting

All users shall address any questions regarding policy, responsibilities, and duties to the BCI/OHLEG Support Center or OHLEG Quality Assurance. If an agency CEO, OAC, or any user either suspects misuse or knows of a violation of OHLEG security policies, it is their duty to take immediate action to contact OHLEG. The agency CEO or OAC may suspend an account at any time if they suspect misuse. If misuse is found, the account should be suspended to prevent further misuse. Additionally, all users shall immediately report to the BCI/OHLEG Support Center any known or suspected security incidents or improper use of OHLEG, whether or not such event resulted in an unauthorized disclosure.

Data Security

4.0 Criminal Justice Information (CJI)

It is the intention of OHLEG to ensure the protection of Criminal Justice Information until such time as the information is either released to the public via authorized dissemination (e.g., within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

CJI shall only be used and disseminated consistent with the authorized purpose for which it was accessed. Dissemination of CJI to another agency is authorized if (a) the other agency is an authorized recipient of such information, or (b) the other agency is performing personnel and appointment functions with codified authority to obtain CJI for criminal justice employment applicants.

The following rules would apply when dealing with OHLEG data:

1. Make printouts unreadable prior to disposal.
2. Before exchanging OHLEG data, agencies must have formal agreements in place that specify security controls.
3. Do not email, transport, or store OHLEG information on electronic media unless it is encrypted.

4.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI) is a subset of CJI. Due to its sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

The dissemination of CHRI to any person outside of the participating agency shall be logged by the participating agency. The following dissemination information shall be logged:

1. Date.
2. Recipient agency and OAI.
3. Record type.
4. Method or means (fax, hard-copy distribution, e-mail, etc.).
5. Person who disseminated.
6. Person who received.

4.2 Personally Identifiable Information (PII)

OHLEG-provided data maintained by an agency, including but not limited to, education, financial transactions, and criminal or employment history may include PII. A criminal history record, for example, inherently contains PII.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

4.3 Dissemination

CJI obtained through OHLEG may not be used or disseminated beyond the implied or expressed consent of the Superintendent of the Bureau of Criminal Investigation. Use and dissemination is deemed to be within the scope of the Superintendent's consent when it is provided to a criminal justice agency or a defendant's counsel, in accordance with dissemination restrictions specified herein at Section 4.4.

4.4 Dissemination of CJI Related to Discovery Motion

CJI obtained through OHLEG routinely becomes a part of investigative case files provided to the county or federal prosecutor. When a prosecutor determines that OHLEG output should be given to defense counsel in response to a demand for discovery under a Rule of Criminal Procedure, a prosecutor may turn the OHLEG output over to defendant's counsel. In such cases, all CJI obtained via OHLEG shall be marked "counsel only." In addition, defense counsel should be advised in writing that "The criminal justice information obtained via the Ohio Law Enforcement Gateway is protected pursuant to ORC 2913.04(D). Dissemination of this information beyond defense counsel is considered a misuse of information obtained via the Ohio Law Enforcement Gateway and will be prosecuted accordingly. Dissemination beyond defense counsel or defense counsel's agents or employees may constitute a violation of Ohio Criminal Rule 16(C) and subject counsel to further disciplinary action."

4.5 CHRI Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

4.6 Passwords

All users acknowledge that it is their responsibility to protect the information contained in OHLEG to the best of their ability and that they are solely responsible for all activities performed under their account. Therefore, users should use unique accounts and passwords for all systems and never share accounts or passwords with any other person or use any other person's accounts and passwords to access any BCI/OHLEG information resource. Users should use screen locks with password protection on all devices used to access BCI/OHLEG information resources. Users shall not share their account(s), passwords, Personal Identification (PIN), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes. Additionally, strong passwords should be used on all devices used to access BCI/OHLEG information resources.

4.7 Physical Protection

The agency must ensure that OHLEG CJI and information system hardware, software, and media are physically protected in a manner and location that does not allow unauthorized persons to view or have access to CJI. Users shall operate systems and technology only in a secure environment and when not in use, they should be secured to ensure that unauthorized access does not occur. This protection should include the following:

1. A secure facility with physical and personnel security controls which allow access only to approved personnel.
2. The location of physical display media such as monitors so that they cannot be viewed by unauthorized personnel.
3. Visitor control that ensures no visitors are left unescorted in areas with access to CJI or information hardware, software, or media.
4. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas shall be subject to state and national fingerprint-based record checks unless these individuals are escorted by authorized personnel at all times.

4.8 Controlled Area

If an agency cannot meet all the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a “controlled area” for the purpose of day-to-day CJI access or storage.

The agency shall at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
 2. Lock the area, room, or storage container when unattended.
 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
- The physical protection standards listed in 4.7 and 4.8 apply to an agency’s physical facility. Please refer to sections 4.11 and 4.12 for rules governing mobile technologies.

4.9 Personally Owned Information Systems

A personally owned computer or other digital device shall not be authorized to access, process, store, or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned computer usage. This control does not apply to the use of personally owned computers to access the agency’s information systems and information that is intended for public access.

4.10 Publicly Accessible Computers

Using publicly accessible computers to access OHLEG is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, and public kiosk computers.

4.11 Mobile Technologies

Cellular telephones, smartphones (e.g., Blackberry, iPhones, etc.), tablets, iPads, laptops, and “air cards” are examples of cellular handheld devices or devices that employ cellular technology. Additionally, cellular handheld devices typically include Bluetooth, Wi-Fi, and other wireless protocols

capable of joining infrastructure networks or creating dynamic ad hoc networks. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to OHLEG.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).

4.12 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

1. Are password protected.
2. Are signed off of OHLEG following each session and before left unattended.
3. Have enabled all existing device security features.

4.13 Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms, whether stored or in transit, is restricted to authorized individuals. Whenever possible, electronic media transported outside of a secured facility

should be encrypted to further protect it from unauthorized access. Physical media shall be protected at the same level as the information would be protected in electronic form.

4.14 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or magnetically erase electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Agencies shall ensure that the sanitization or destruction is witnessed or carried out by authorized personnel. Destruction should be documented and logged.

4.15 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information being compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure that the disposal or destruction is witnessed or carried out by authorized personnel. Bulk destruction of protection media performed by third party contractors should be documented and logged.

Technical Compliance

5.0 Device and Resource Protection Guidelines

1. Agency management shall ensure that any computer and/or network used to access AGO/BCI/OHLEG information resources does not contain security tools that could be directed to AGO/BCI/OHLEG information resources. Security tools are those used to perform analysis of vulnerabilities in computer systems as well as simulate network or computer attacks that could be detrimental to OHLEG.
2. Agency management shall acknowledge that OHLEG management reserves the right to deny the agency access to AGO/BCI/OHLEG information resources if an event is noted that could potentially put the AGO/BCI/OHLEG information resources or data at risk.

3. Agency shall take reasonable measures to ensure that the agency network and all devices accessing AGO/BCI/OHLEG information resources are secure and free from malicious code.
4. Agency shall have a documented Security Policy that includes but is not limited to the following standards: password controls; user account activation and deactivation process; Incident Process and Procedure; and requirements for end point and perimeter protection, which include but are not limited to the following measures: Antivirus Software, Anti-malware Software, Disk Encryption, Personal Computer Firewalls, Personal Computer Intrusion Detection Software and Intrusion Prevention Software.
5. Agency management shall consent to requests for review of any equipment used to access AGO Information Resources.
6. Agency shall consent to review of security controls or provide adequate documentation upon request.
7. All devices used to access AGO/BCI/OHLEG information resources shall have up-to-date antivirus software running at all times, employ the use of firewalls and have all security related operating system patches applied, and supported internet browser versions installed and updated with all vendor security patches. BCI/OHLEG and/or AGO ITS administration reserves the right to deny access to any device that does not comply.
8. Users shall not download, install, or run security programs or utilities including but not limited to password cracking programs, packet sniffers, or port scanners that attempt to reveal or exploit weaknesses in the security of an AGO/BCI/OHLEG information resource unless approved by AGO ITS Security.
9. Users shall not use shareware or freeware software without the appropriate management approval from their respective agency. Any such software must not permit access to any AGO/BCI/OHLEG data or resources.
10. Users shall not make unauthorized copies of AGO/BCI/OHLEG-owned software, data, or attributes.

11. Users shall not engage in activity that may degrade the performance of AGO/BCI/OHLEG information resources; deprive an OHLEG user access to AGO/BCI/OHLEG information resources; obtain extra resources beyond those allocated; or circumvent AGO/BCI/OHLEG information resources security measures.

5.1 Data Security Threat Incident Response

Agencies shall track and document malicious computer attacks and report such attacks to the BCI/OHLEG Support Center. The OHLEG OAC shall:

1. Be the primary point of contact for interfacing with OHLEG concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Establish procedure for incident reporting in their absence.

Additionally, users shall report any known weaknesses in computer security to the appropriate agency security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.

Appendix A: OHLEG Practice and Test Inquiries

Vehicles:

License Plate #s – TST0001 through TST0069

Ohio BMV Driver's License Records:

SSN – 777-77-7775

OLN – ZZ000000, ZZ000015, ZZ000083

Ohio BMV Image Records:

OLN – ZZ0000007 and ZZ000520

BCI CCH Test Record:

Name – Public, John Q

Sex – Male

Race – White

DOB – 12/11/1946

BCI# – A123456

Appendix B: Model OHLEG Policy

Agencies are strongly encouraged to develop their own policies to augment the OHLEG security policies. The following are suggested policy statements for an OHLEG Participating Agency's supplemental OHLEG policy. The term CEO refers to an agency's highest ranking administrative official such as a police chief or sheriff. This model policy is available so that each user agency can have an example to reference as it fits these procedures and terminology into the agency's current structure and directives.

The following agency rules apply to the use of OHLEG by any agency member.

The Ohio Attorney General's Office grants agencies and individuals the access to and use of OHLEG exclusively for criminal justice purposes. By virtue of user agreements, the Smallville Police Department and its officers agree to the strict adherence to OHLEG security policies. Individual non-compliance with OHLEG security policies can result in loss of OHLEG access not only for the individual but also potentially for the entire agency. In order to ensure compliance with OHLEG rules and proper usage the Smallville Police Department has created this OHLEG use policy. This OHLEG policy is meant to supplement the existing OHLEG security policies. If there is any question of conflict with the OHLEG rules, the most restrictive interpretation of the OHLEG rules should be applied.

OHLEG use is governed by provisions of the Ohio Revised Code and by the OHLEG security policies (Ohio Rev. Code §§109.57 and 2913.04). Any violations of these rules or misuse or abuse of OHLEG privileges by any member of the Smallville Police Department will be considered a serious violation of agency policy and result in disciplinary action up to and including termination of employment. In addition, violations of the Ohio Revised Code will be referred to the appropriate county prosecutor for criminal prosecution.

In order for any employee at the Smallville Police Department to obtain OHLEG access, the individual must first watch the OHLEG Security Training Video and then submit a request for OHLEG access in writing to his or her supervisor. The supervisor—or an existing OHLEG user—will then fill out an OHLEG application for the individual through the OHLEG Online Account Application process. The applicant will then be required to personally enter his or her name, social security number, and date of birth. The application will then go to the Agency Approver, who will ensure the individual has watched the OHLEG Security Training Video

and signed the OHLEG Agency/User Agreement, select which attributes the individual should have access to, and send the application to the BCI/OHLEG Support Center. Once the individual's application is approved, he or she will be able to access OHLEG.

A copy of the OHLEG security policies will be made available to all approved users of OHLEG. These rules are not for public dissemination and must not leave the agency facility. OHLEG users will be held responsible for understanding the contents of the OHLEG security policies, as well as for applying these rules in their use of OHLEG. Agency users will be required to sign a statement indicating they have read and understand the OHLEG security policies before being granted OHLEG access.

OHLEG user authorizations are granted to individual agency members for their exclusive use. All OHLEG transactions are monitored by BCI and subject to audit procedures to verify proper usage and detect violations. Agency members are prohibited from:

- 1) Allowing any unauthorized person to access OHLEG;
- 2) Sharing or giving their sign-on credentials to any other person;
- 3) Leaving their sign-on credentials unprotected in such a way that another person might obtain them; and
- 4) Leaving a computer which has open access to OHLEG unattended and available to unauthorized personnel.

The use of OHLEG is strictly limited to criminal justice purposes. Agency members will be granted access to specific OHLEG attributes based on the particular needs of their job assignment.

Use of OHLEG for anything other than a criminal justice purpose is strictly forbidden. An OHLEG user is not permitted to use an attribute for which he or she has not been given access. Criminal Justice Information (CJI) obtained through OHLEG is also protected and is not to be shared with any unauthorized person.

The agency's OHLEG Agency Coordinator (OAC) is responsible for assisting the CEO with overseeing compliance with OHLEG security policies.

OHLEG access is not permitted outside of normal working hours unless specifically authorized by the OAC.

OHLEG access is not permitted from non-agency computers unless specifically authorized by the OAC.

Anyone becoming aware of an agency member using OHLEG in violation of agency or OHLEG security policies, or in a manner inconsistent with state or federal law, shall report said violation to a superior officer as soon as possible.

If an agency member becomes aware of themselves having committed an OHLEG violation, they are to self-report the violation to their supervisor and the OAC so the violation can be documented. The circumstances that gave rise to the violation can then be examined to determine if there is a need for additional training. Self-reporting a violation does not relieve the user from responsibility for committing the violation.

All OHLEG violations will be reported to the BCI/OHLEG Support Center by either the CEO or OAC.

Any OHLEG violations that rise to the level of a criminal offense will be investigated by the agency, BCI, and/or such outside agencies as deemed appropriate. The results of said investigation will be referred to the county prosecutor for consideration of criminal charges. Violations of the OHLEG restrictions in the Ohio Revised Code are a fifth degree felony.

The OAC shall be responsible for training, applications, policy oversight, and internal audits. Internal audits will be conducted (monthly, quarterly, on an ongoing basis) with a copy of said audit results kept on file in the CEO's office. All violations of this agency policy, OHLEG rules, or Ohio law will be reported to the CEO. The report will include a description of the violation, frequency of occurrence, immediate steps taken to correct the situation, mitigating factors, and an indication of whether additional agency or individual training is needed. The violation and a report on agency action will be forwarded to OHLEG.

Access to OHLEG is a job-specific authorization. Consequently, if an OHLEG user is promoted, transferred, or otherwise experiences a change in duties, they must notify the OAC as soon as possible so the level of their OHLEG authorizations can

be evaluated in light of their new assignment. If a member is terminated, their ability to lawfully access OHLEG is immediately ended, and they are prohibited from accessing OHLEG for any reason. If a member is suspended from duty, they are not permitted to access OHLEG for any reason until such time as they are reinstated to full duty status. If a member is off duty due to sickness, injury, or disability, they are not to access OHLEG for any reason without receiving authorization from the OAC.

Appendix C: Referenced Ohio Revised Code

OHLEG Relevant Sections of Ohio Revised Code

109.57 Duties of superintendent

(C)(1) The superintendent may operate a center for electronic, automated, or other data processing for the storage and retrieval of information, data, and statistics pertaining to criminals and to children under eighteen years of age who are adjudicated delinquent children for committing an act that would be a felony or an offense of violence if committed by an adult, criminal activity, crime prevention, law enforcement, and criminal justice, and may establish and operate a statewide communications network to be known as the Ohio law enforcement gateway to gather and disseminate information, data, and statistics for the use of law enforcement agencies and for other uses specified in this division. The superintendent may gather, store, retrieve, and disseminate information, data, and statistics that pertain to children who are under eighteen years of age and that are gathered pursuant to sections 109.57 to 109.61 of the Revised Code together with information, data, and statistics that pertain to adults and that are gathered pursuant to those sections.

(4) The attorney general may adopt rules under Chapter 119. of the Revised Code establishing guidelines for the operation of and participation in the Ohio law enforcement gateway. The rules may include criteria for granting and restricting access to information gathered and disseminated through the Ohio law enforcement gateway. The attorney general shall permit the state medical board and board of nursing to access and view, but not alter, information gathered and disseminated through the Ohio law enforcement gateway.

The attorney general may appoint a steering committee to advise the attorney general in the operation of the Ohio law enforcement gateway that is comprised of persons who are representatives of the criminal justice agencies in this state that use the Ohio law enforcement gateway and is chaired by the superintendent or the superintendent's designee.

(D)(1) The following are not public records under section 149.43 of the Revised Code: (b) Information, data, and statistics gathered or disseminated through the Ohio law enforcement gateway pursuant to division (C)(1) of this section...

<http://codes.ohio.gov/orc/109.57>

2913.04 Unauthorized use of property - computer, cable, or telecommunication property

(D) No person shall knowingly gain access to, attempt to gain access to, cause access to be granted to, or disseminate information gained from access to the Ohio law enforcement gateway established and operated pursuant to division (C)(1) of section 109.57 of the Revised Code without the consent of, or beyond the scope of the express or implied consent of, the superintendent of the bureau of criminal identification and investigation.

(I) Whoever violates division (D) of this section is guilty of unauthorized use of the Ohio law enforcement gateway, a felony of the fifth degree.

<http://codes.ohio.gov/orc/2913.04>

149.433 Exempting security and infrastructure records.

(A)(3) "Security record" means any of the following: (a) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage...

(B) A record kept by a public office that is a security record or an infrastructure record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

<http://codes.ohio.gov/orc/149.433>

109.88 Investigation of telecommunications and telemarketing fraud.

(A) If the attorney general has reasonable cause to believe that a person or enterprise has engaged in, is engaging in, or is preparing to engage in a violation of any provision of section 2913.04 or 2913.05 of the Revised Code, the attorney general may investigate the alleged violation.

<http://codes.ohio.gov/orc/109.88>